PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-033756
(43)Date of publication of application : 31.01.2002

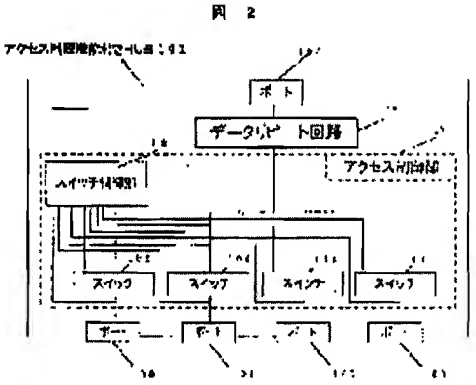
(51)Int.Cl. H04L 12/44

(21)Application number : 2000-218711
(22)Date of filing : 14.07.2000

(71)Applicant : HITACHI LTD
(72)Inventor : KODA SHUSAKU
TSURUTA HIROSHI

(54) HUB WITH ACCESS LIMIT FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To solve the problems that conventionally a HUB, to which terminals are connected via routers, that the enhancement of the security of each terminal is indispensable to ensure the security of the terminals connected to the same HUB via the routers, that the security of all the terminals are endangered, once a manager right of the terminals is deprived, that the grouping of the terminals which are not communicating with each other into separate segments be required as the countermeasures and that expensive routers be required, when the number of the terminals increases resulting in complicated security rules described in the routers.
SOLUTION: The HUB itself is provided with a function, by which the direction and destination of data carried through each port can be discriminated to attain only communications between limited ports. Thus, by building up a scheme which will not to affect other terminals, even if the manager right of a terminal is deprived, the security for the terminals can be managed with few number of routers and without interactions occurring within the same segment.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－33756
（P2002－33756A）
(43)公開日　平成14年１月31日(2002.1.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/44		Ｈ０４Ｌ　11/00	３４０	５Ｋ０３３

審査請求　未請求　請求項の数１　ＯＬ　（全５頁）

(21)出願番号　特願2000－218711(P2000－218711)

(22)出願日　平成12年７月14日(2000.7.14)

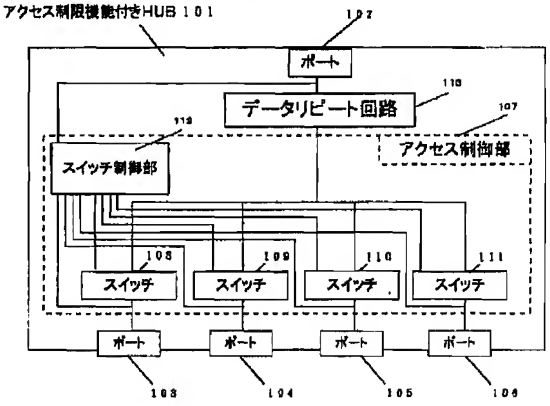
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　好田　秀作
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバー事業部内
(72)発明者　▲鶴▼田　啓
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバー事業部内
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　5K033 CB08 DB03 DB18

(54)【発明の名称】　アクセス制限機能付きＨＵＢ

(57)【要約】
【課題】ルータ経由で同一ＨＵＢに接続された端末のセキュリティ確保には、各端末のセキュリティの向上が不可欠であり、一旦端末の管理者権限が奪われるとその場の端末全てが危険にさらされる。この対策として相互に通信をしない端末同士は、ルータで個別のセグメントに分ける必要が有った。また、端末の台数が増えてくると高価なルータが必要になりそこに記述するセキュリティルールも複雑なものになる。
【解決手段】ＨＵＢ自体に各ポートを流れるデータの方向と行き先が判断できる機能を備え、限られたポート間の通信のみを可能にする。これにより、ある端末の管理者権限が奪われても、他の端末に影響を及ぼさない仕組みを構築することで、少ないルータで且つ、同一セグメントでの相互作用しない端末のセキュリティ管理が可能になる。

図　2



1

【特許請求の範囲】
【請求項１】　複数のポートと、各ポート間のデータを中継するためのデータリピート回路とを備えるＨＵＢにおいて、特定のポート間の通信のみ許可し、その他のポートとの通信を阻止する機能を有するアクセス制限機能付きＨＵＢ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ローカルエリアネットワーク（ＬＡＮ）において、複数の端末の間でデータを中継するために利用されるＨＵＢに関するものであり、さらに詳しくは、特定のポート間の通信を制限することで、個々の端末のセキュリティを高めることができるＨＵＢに関するものである。
【０００２】
【従来の技術】従来、ＬＡＮにおいてセキュリティ性を高める方法としては、ゲートウエイ(ファイアウォールを含む)、ルータやレイヤ３スイッチのアクセス制限機能により、特定のアドレスを持つ端末の通信を制御する方法が用いられている。図１はアクセス制限機能を有するゲートウエイ(ファイアウォールを含む)、ルータやレイヤ３スイッチの動作を示している。ゲートウエイ(ファイアウォールを含む)、ルータやレイヤ３スイッチに、端末の論理アドレス(例ＩＰアドレス)と通信の許可・不許可を定義したアクセスリストを管理者が登録する。ゲートウエイ(ファイアウォールを含む)，ルータやレイヤ３スイッチはアクセスリスト中で、許可された通信のみを転送する。今、ポートＰＡに接続されたアドレスＡを有する端末Taと、ポートPBに接続れたアドレスＢを有する端末Tb間の通信は許可し、且つ、端末TbとポートPCアドレスCを有する端末Tcとの通信は不許可としたいとする。管理者は通信を許可する端末のアドレスと通信の許可・不許可を定義したアクセスリストを、あらかじめルータやレイヤ３スイッチに登録しておかなくてはならない。さらにこのとき、各ポートに別々の論理ネットワークグループを設定する必要がある。
【０００３】
【発明が解決しようとする課題】上述のように、ゲートウエイ(ファイアウォールを含む)、ルータやレイヤ3スイッチのアクセス制御機能を利用した方法は、設定の変更により柔軟にアクセス制限を定義できる利点がある。しかし、製品が高価であるという欠点を持っているうえに、ネットワークの構成が変わった場合などに、物理的な接続を変更する上にアクセス制限の設定を変更する作業が必要であるという煩わしさがともなう。
【０００４】本発明は上述のような点に鑑みてなされたものであり、その目的とするところは、低コストでアクセスリスト作成の煩雑さが少なく、管理者権限を不正入手されることが無いアクセス制限機器を提供することにある。

2

【０００５】
【課題を解決するための手段】本発明にあっては、上記の課題を解決するために、図２に示すように、複数のポート１０２，１０３，１０４，１０５，１０６と、各ポート間のデータを中継するためのデータリピート回路１１３とを備えるＨＵＢ１０１において、各ポートのデータを中継するかしないかを制御するアクセス制御部１０７を有するものである。本発明の図２によれば、アクセス制御部１０７が、アクセス制限機能付きＨＵＢ１０１の各ポート１０３～１０６に接続される。アクセス制御部１０７は、ポート１０３～１０６と通信できるポート１０２と、ポート１０２とのみ通信できるポート１０３～１０６間の通信のみ転送する。また、その他のポート１０３～１０６間通信は転送しないよう動作することにより、特定のポート以外との通信ができないようにするものである。これにより、ユーザ（管理者）は端末のアドレスの登録や削除を一切行うことなく、アクセス制限を行うことができるものである。
【０００６】
【発明の実施の形態】（実施形態１）図２は本発明の一実施例のブロック図である。それぞれのポート１０３～１０６毎にアクセス制御機構としてスイッチ１０８～１１１が接続されており、スイッチ１０８～１１１にはスイッチの動作を制御するスイッチ制御部１１２が接続されている。ポート１０３，１０４，１０５，又は１０６からポート１０２に向けてデータが流れる場合について動作を説明する。ポート１０３，１０４，１０５，又は１０６に受け取られたデータは、それぞれスイッチ１０８、１０９，１１０、または１１１で受取られると共にスイッチ制御部１１２に受け取られる。スイッチ制御部１１２はデータを受け取ったポートを識別し、データを受け取ったポートと接続されたスイッチを接続状態とし、それ以外のポートに接続されたスイッチを切断状態とする。これによりデータリピート回路１１３のみにデータを送る。データリピート回路はポート１０２にデータを送る。次にポート１０２からポート１０３，１０４，１０５，又は１０６に向けてデータが流れる場合について動作を説明する。ポート１０２が受け取ったデータは、データリピート回路１１３を介して全てのスイッチ１０８～１１１に送られ、そのままポート１０３～１０６データが流れる。また、ポート１０２に流れたデータは、データリピート回路１１３を介して全てのスイッチ１０８～１１１に送られ、ポート１０３，１０４，１０５，及び１０６に流れる。
【０００７】図３は本実施例の動作説明図である。ポート１０２は他のすべてのポート１０３～１０６と通信可能であり、ポート１０３～１０６はポート１０２とのみ通信可能なポートである。例えば、ポート１０２からデータが送信されると図２のスイッチ１０８～１１１がすべてＯＮになり、すべてのポートと通信可能となる。ポ

ート１０３にデータが送信されると、スイッチ１０８のみがＯＮになり、ポート１０２とのみ通信可能となる。

【０００８】（実施形態２）本発明のその他の一実施例について説明する。図２のブロック図において、それぞれのポート１０３～１０６毎にアクセス制御機構としてスイッチ１０８～１１１が接続されており、スイッチ１０８～１１１にはスイッチの動作を制御するスイッチ制御部１１２が接続されている。ポート１０３，１０４，１０５，又は１０６からポート１０２に向けてデータが流れる場合について動作を説明する。ポート１０３，１０４，１０５，又は１０６に受け取られたデータは、それぞれスイッチ１０８、１０９，１１０、または１１１で受取られると共にスイッチ制御部１１２に受け取られる。スイッチ制御部１１２はデータを受け取ったポートを識別し、データを受け取ったポートと接続されたスイッチを接続状態とし、それ以外のポートに接続されたスイッチを切断状態とする。これによりデータリピート回路１１３のみにデータを送る。データリピート回路はポート１０２にデータを送る。次にポート１０２からポート１０３，１０４，１０５，又は１０６に向けてデータが流れる場合について動作を説明する。ポート１０２が受け取ったデータは、スイッチ制御部１１２で宛先のポート１０３，１０４，１０５，又は１０６をチェックされ、該当するポートに接続されたスイッチのみを接続状態とし、それ以外のポートに接続されたスイッチを切断状態にすることにより、該当ポートのみに送られ、どのポート１０３～１０６にも該当しない場合そのデータは捨てられる。

【０００９】（実施形態３）図４は、スイッチングＨＵＢの応用によるアクセス制限機能付きＨＵＢ２０１である。各ポート２０２～２０６に対し各々を認識可能なアドレスを付加する、２０２～２０６に接続されていない外部からコントロールポート２０７に接続しアクセス制御部２０８にセキュリティポリシーを記述する。

【００１０】アクセス制御部２０８は、アクセス制限機能付きＨＵＢ２０１の各ポート２０２～２０６を付加されたアドレスで認識しセキュリティポリシー設定された上で通信可能ポートだけのデータのやり取りを可能とする。コントロールポート２０７は、その他のいかなるポート２０２～２０６とも通信は出来ない。

【００１１】本システムでは、ＣＰＵ、メモリ等を設置し各ポート２０２～２０６に流れるデータを抽出し、ＴＣＰ／ＩＰのプロトコルを例に取れば発信元ＴＣＰ、ＵＤＰポート番号と発信先ＴＣＰ、ＵＤＰポート番号をチェックしパケットフィルタ型のファイアウォールの構築も可能になる。

【００１２】

【発明の効果】本発明によれば、複数のポート間でデータを中継するためのＨＵＢにおいて、特定のポート間の通信のみ許可し、その他のポートとの通信を阻止する機能を有するアクセス制限機能を持たせることにより、ユーザによるアクセスリストの管理の必要を無くすことができ、また、特定のポートとの通信のみを許可することで、セキュリティ性を高めることができ、ルータやスイッチのアクセス制限機能を用いる方法より低コストで実現でき、ルータやスイッチの管理者権限を第三者に不正入手されることが無いという効果がある。インターネットに接続されたサーバでの設定例を元に効果の具体例を示す。

【００１３】図５(ａ)では、端末がインターネットに提供しているサービスのアプリケーションにセキュリティ上の欠陥があり、端末の1つが管理者権限を奪われた場合、ＨＵＢの場合その他の端末も危険にさらされる。

【００１４】この時ファイアウォールもしくはルータは何の役にも立たない。ＨＵＢ接続されているイーサネット（登録商標）の速度で、攻撃が行われる。この対策としては個々に端末のセキュリティを向上させるしかない。技術的に高度であるし、台数分のセキュリティ対策が必要な為時間も掛かる。また、端末を直接操作できるサービスを提供していては、上記の環境では、他の端末に対し自由にアクセスできてしまう。図５(ｂ)は図５(ａ)の対策型である。インターネットから端末に対してのアクセスを許可したい場合、セキュリティを考慮すると、各サービス毎にネットワークグループをファイアウォールもしくはルータで分割する必要がある。この場合、たとえ端末が乗っ取られた場合でも他の端末に影響を与えない。ネットワークグループ毎に、ネットワークインタフェースを設ける時ネットワークインタフェースの数は物理的に限界がある。

【００１５】図５(ｃ)は、アクセス制限機能付きＨＵＢで構築した場合である。アクセス制限機能付きＨＵＢは端末からファイアウォールもしくはルータに対してのアクセスを許可しても端末同士のアクセスを物理的に止めてしまう。インターネットから端末に対してのアクセスを許可したい場合、ルータやファイアウォールでアクセスコントロールを施せば、セキュリティＨＵＢに接続されている端末が乗っ取られた場合でもセキュリティＨＵＢを跨って、他の端末には攻撃が出来ない。また、ネットワークグループ毎に、ネットワークインタフェースを設ける必要が無い為コストが少なくて済む。

【図面の簡単な説明】

【図１】従来例の動作説明図である。

【図２】本発明の一実施例のブロック図である。

【図３】本発明の一実施例の動作説明図である。

【図４】スイッチングＨＵＢを応用したアクセス制限機能付きＨＵＢを示す図である。

【図５】アクセス制限機能付きＨＵＢの使用例を示す図である。

【符号の説明】

１０１…アクセス制限機能付きＨＵＢ、１０２～１０６

5

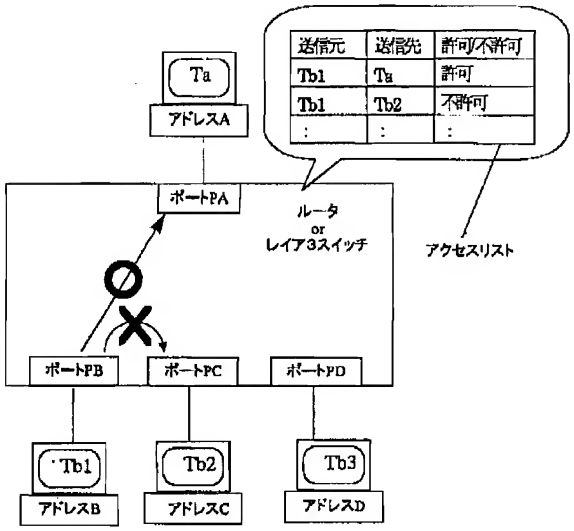
…ＨＵＢのポート、１０７…各ポートのデータの流れを制御するアクセス制御部、１０８～１１１…ＨＵＢのポート１０３～１０６に流れるデータ処理するスイッチ、１１２…スイッチに流れたデータを制御するスイッチ制御部、１１３…データリピート回路、２０１…アクセス＊

6

＊制限機能付きＨＵＢ、２０２～２０６…ＨＵＢのポート、２０７…アクセス制御部を外部装置から制御するポート、２０８…ＨＵＢのポートに流れるデータを制御するアクセス制御部。

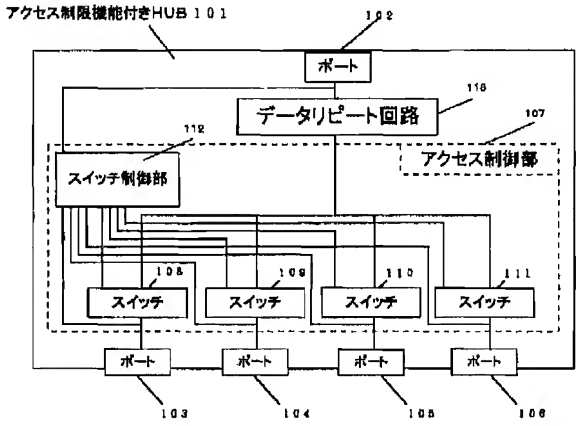
【図１】

図　1



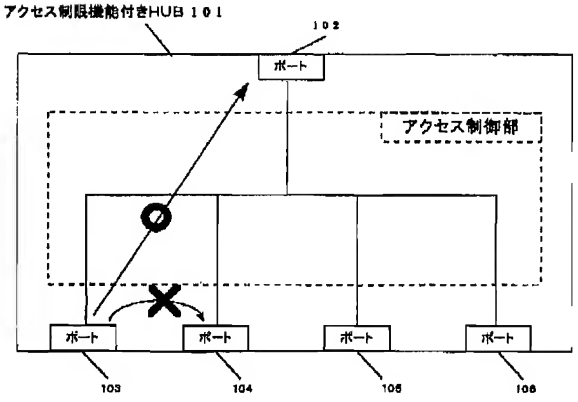
【図２】

図　2



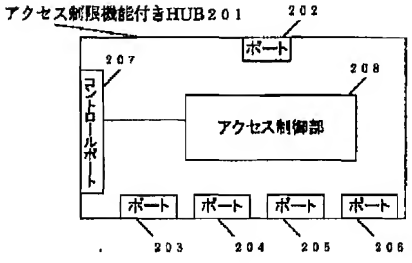
【図３】

図　3



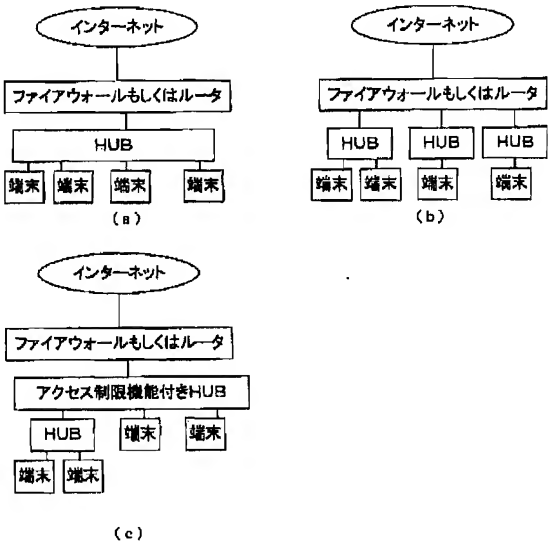
【図４】

図　4



【図５】

図 5


インターネット
ファイアウォールもしくはルータ
HUB
端末
端末
端末
端末
(a)
インターネット
ファイアウォールもしくはルータ
HUB
HUB
HUB
端末
端末
端末
端末
(b)
インターネット
ファイアウォールもしくはルータ
アクセス制限機能付きHUB
HUB
端末
端末
端末
端末
(c)